

# On higher congruences between cusp forms and Eisenstein series

Bartosz Naskręcki

**Abstract** In this paper we present several finite families of congruences between cusp forms and Eisenstein series of higher weights at powers of prime ideals. We formulate a conjecture which describes properties of the prime ideals and their relation to the weights. We check the validity of the conjecture on several numerical examples.

## 1 Introduction

In this paper we present new numerical data concerning congruences between cusp forms and Eisenstein series.

Let  $p$  be a rational prime. For a newform  $f \in \mathcal{S}_k(\Gamma_0(p))$ , let  $K_f = \mathbb{Q}(\{a_n(f)\}_{n \geq 0})$  be the field generated by the Fourier coefficients of the form  $f$  and let  $\mathcal{O}_f$  be its ring of integers. Let  $E_k$  denote the Eisenstein series of weight  $k$  given by the  $q$ -expansion  $-\frac{B_k}{2k} + \sum_{n=1}^{\infty} (\sum_{d|n} d^{k-1}) q^n$ , where  $B_k$  is the  $k$ -th Bernoulli number. We define the series  $E_k^{(p)}$  by  $E_k^{(p)}(\tau) = E_k(p\tau)$ . From the theorem of Mazur [11, Proposition 5.12, Proposition 9.6] we know that for  $k = 2$  and for any fixed prime  $p \geq 11$  if we choose any prime  $\ell \neq 2, 3$  dividing the numerator of the zeroth coefficient of the Eisenstein series  $E_2 - pE_2^{(p)}$  of weight 2, then there exists a newform  $f$  in  $\mathcal{S}_2(\Gamma_0(p))$  and a maximal ideal  $\lambda \in \mathcal{O}$  above  $\ell$  such that

$$a_r(f) \equiv a_r(E_2 - pE_2^{(p)}) \pmod{\lambda} \quad (1)$$

for almost all primes  $r$ .

---

Bartosz Naskręcki  
Graduate School, Faculty of Mathematics and Computer Science, Adam Mickiewicz University,  
Poznań, Poland, e-mail: bartnas@amu.edu.pl

We study a generalization of the congruence (1), when the coefficients of modular forms lie in number fields and deal with prime ideals coprime with the level.

Choose  $E = E_k - p^{k-1}E_k^{(p)}$ . Assume there exists a newform  $f \in \mathcal{S}_k(\Gamma_0(p))$ , a natural number  $r \geq 1$  and a maximal ideal  $\lambda \in \mathcal{O}_f$ , such that

$$a_n(E) \equiv a_n(f) \pmod{\lambda^r} \quad (2)$$

for all  $n \geq 0$ . Let  $\ell$  be the rational prime below  $\lambda$  and  $p \notin \lambda$ . Then  $\ell$  divides the numerator of  $a_0(E)$ . More precisely,

$$r \leq \text{ord}_\lambda\left(\frac{-B_k}{2k}(1-p)\right),$$

where  $B_k$  is a  $k$ -th Bernoulli number. This is proved in Corollary 1 and Lemma 1. In the proof, we use the explicit description of  $a_p(f)$  for a newform  $f \in \mathcal{S}_k(\Gamma_0(p))$ , cf. [1, Theorem 3].

In the range of our computations we found several numerical examples such that  $r = \text{ord}_\lambda\left(\frac{-B_k}{2k}(1-p)\right)$  when  $\text{ord}_\lambda(\ell) = 1$ , cf. Table 3. On the other hand, if the prime ideal  $\lambda$  is ramified, i.e.  $\text{ord}_\lambda(\ell) > 1$  and  $\ell > 2$ , then the situation is a bit different. On the basis of numerical evidence we found that for all computed cases, the upper bound for the exponent of the congruence (2) is equal to the ramification index  $\text{ord}_\lambda(\ell)$ . Hence we propose the following conjecture.

*Conjecture 1.* Let  $k \geq 2$  and  $p \geq 3$  be a prime number. Choose  $E = E_k - p^{k-1}E_k^{(p)}$ , where  $E_k^{(p)}(\tau) = E_k(p\tau)$ . Assume there exists a newform  $f \in \mathcal{S}_k(\Gamma_0(p))$ , a natural number  $r \geq 1$  and a maximal ideal  $\lambda \in \mathcal{O}_f$ , such that

$$a_n(E) \equiv a_n(f) \pmod{\lambda^r} \quad (3)$$

for all  $n \geq 0$ . Let  $\ell$  be the rational prime below  $\lambda$ . If  $\ell > 2$  and  $\text{ord}_\lambda(\ell) > 1$ , then

$$r \leq \text{ord}_\lambda(\ell).$$

The symbol  $\text{ord}_\lambda$  denotes the  $\lambda$ -valuation which is normalized by  $\text{ord}_\lambda(\lambda) = 1$ .

The conclusion of the conjecture is false for  $\ell = 2$ . For example, there is a Galois conjugacy class of newforms in  $\mathcal{S}_2(\Gamma_0(257))$  such that the representative is congruent to the Eisenstein series  $E_2 - 257E_2^{(257)}$  modulo  $\lambda^5$  for a prime  $\lambda$  above 2 such that  $\text{ord}_\lambda(2) = 2$  (cf. Table 4).

The special case of congruences between newforms and Eisenstein series leads to the following question.

*Is it true that for prime  $\ell > 3$  there is at most one newform, up to Galois conjugacy, congruent to a fixed Eisenstein series ?*

We found several examples which show that the answer to the above question is negative for  $\ell = 2$ ,  $\ell = 3$  and some properly chosen ideal  $\lambda$  above  $\ell$ . For example,

take prime level  $p = 353$ . The space  $\mathcal{S}_2(\Gamma_0(353))$  has dimension 29 and 4 different Galois conjugacy classes of newforms. With respect to the internal MAGMA numbering, the first, second and fourth Galois conjugacy classes contain a newform congruent to the Eisenstein series  $E_2 - pE_2^{(p)}$ . For  $\ell = 3$ , we can take  $p = 487$  and find newforms congruent to the Eisenstein series in Galois conjugacy classes with numbers 2 and 4. Mazur indicates that there may be infinitely many such examples for  $\ell = 2$ , cf. [11, II.19].

Our motivation to study the congruences (2) comes from the question posed in [8, Paragraph 4.4]. The authors study congruences

$$a_n(f) \equiv a_n(E) \pmod{\lambda^r},$$

for almost all prime indices  $n$ , between a newform  $f \in \mathcal{S}_2(\Gamma_0(p))$  and an Eisenstein series  $E \in \mathcal{E}_2(\Gamma_0(p))$ . Our approach is more restrictive, since we take into account in the congruences all indices  $n \geq 0$ . In this context, the numerical results presented in Section 6 suggest that the general answer to [8, Question 4.1] is yes, even in this more restrictive setting. We find for most of the considered examples only one Galois conjugacy class of newforms which satisfies a congruence of the above type. The value of the exponent  $r$  in many cases equals the upper bound  $\text{ord}_\lambda(-\frac{1}{24}(1-p))$  (here we assume  $\ell > 2$ ). The authors in [8] do not distinguish the situation when the prime ideal  $\lambda$  is ramified or not. In our computational range, if  $\lambda$  is ramified over  $\ell$ , we find that the exponent  $r$  is bounded as in Conjecture 1 but not by the number  $\text{ord}_\lambda(-\frac{1}{24}(1-p))$ , cf. Table 4.

It would be desirable to extend the computations to take into account the situation when the cusp form is of weight  $k_1$  and the Eisenstein series is of weight  $k_2$ , for  $k_1 \neq k_2$ . Such a computational and theoretical study was done for two cusp forms in [4]. Unfortunately, we cannot apply directly the results of the paper [4] to our situation.

The proposed upper bound for  $r$  in Conjecture 1 might be linked to the behavior of the inertia group at  $p$  of the residually reducible Galois representation attached to the newform  $f$ . Such a condition is given in [7, Theorem 2], where the authors deal with congruences between two cusp forms.

In Section 2 we introduce basic notation and describe Hecke algebras and eigenforms. Next, in Section 3 we describe the upper bound for the exponent of congruences between cuspidal eigenforms and Eisenstein series.

In Section 4 for the convenience of the reader we collected basic facts of the theory of  $\ell$ -maximal orders which is an important ingredient of our algorithm. These facts are crucial for several improvements of the algorithm speed.

Section 5 contains a pseudo code description of the main algorithm which was implemented in MAGMA [2]. The source code is available on the request or online, cf. [13].

Section 6 is devoted to presentation of the numerical data which supports the conjecture. We discuss several explicit examples and the numerical data collected in the tables.

## 2 Notation and definitions

Let  $p$  be a prime number and  $k$  a positive even integer. The space  $\mathcal{M}_k(\Gamma_0(p))$  of holomorphic modular forms of weight  $k$  splits over  $\mathbb{C}$  into a direct sum

$$\mathcal{M}_k(\Gamma_0(p)) = \mathcal{E}_k(\Gamma_0(p)) \oplus \mathcal{S}_k(\Gamma_0(p))$$

of the Eisenstein part and the space of cuspidal modular forms (cf.[6, Paragraph 5.11]). From dimension formulas for modular forms we have

$$\dim_{\mathbb{C}}(\mathcal{E}_k(\Gamma_0(p))) = \begin{cases} 1, & k = 2 \\ 2, & k \geq 4. \end{cases}$$

Let  $\sigma_r(n) = \sum_{d|n} d^r$  and  $q = e^{2\pi i\tau}$ , where  $\tau$  lies on the complex upper half-plane  $\mathcal{H}$ . When  $k \geq 2$  we define

$$E_k(\tau) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n.$$

The sequence of Bernoulli numbers  $\{B_m\}_{m \in \mathbb{N}}$  is defined as usual by the series  $\sum_{m=0}^{\infty} B_m t^m = \frac{t}{e^t - 1}$ . Explicitly, in  $\mathcal{E}_2(\Gamma_0(p))$  we have a generator

$$E_2(\tau) - pE_2(p\tau) = \frac{p-1}{24} + \sum_{n=1}^{\infty} \sigma_1(n)q^n - p \sum_{n=1}^{\infty} \sigma_1(n)q^{pn}.$$

The space  $\mathcal{E}_k(\Gamma_0(p))$  is generated by  $E_k(\tau)$  and  $E_k(p\tau)$ .

The space of modular forms  $\mathcal{M}_k(\Gamma_0(p))$  carries a natural action of a commutative  $\mathbb{C}$ -algebra  $\mathbb{T}$  generated by the Hecke operators, cf.[6, Proposition 5.2.1]. The algebra is generated by two types of operators. The first type is defined for the primes  $\ell \neq p$  by the formula

$$T_{\ell}(f) = \sum_{n=0}^{\infty} a_{n\ell}(f)q^n + \ell^{k-1} \sum_{n=0}^{\infty} a_n(f)q^{n\ell},$$

where  $f \in \mathcal{M}_k(\Gamma_0(p))$  and  $a_n(f)$  denotes the  $n$ -th Fourier coefficient of the form  $f$  at infinity. For  $\ell = p$  there is a single operator

$$T_p(f) = \sum_{n=0}^{\infty} a_{np}(f)q^n.$$

We denote by  $\mathbb{T}$  the algebra  $\mathbb{C}[\{T_r\}]$  generated by the Hecke operators  $T_r$ , where  $r$  runs through all rational primes. The action of Hecke algebra  $\mathbb{T}$  on the space  $\mathcal{M}_k(\Gamma_0(p)) = \mathcal{E}_k(\Gamma_0(p)) \oplus \mathcal{S}_k(\Gamma_0(p))$  preserves the direct sum splitting into Eisenstein and cuspidal parts. For  $k = 2$  since  $\dim \mathcal{E}_2(\Gamma_0(p)) = 1$ , the series  $E_2 - pE_2^{(p)}$  is the normalized eigenform.

For  $k \geq 4$  the dimension of the space  $\mathcal{E}_k(\Gamma_0(p))$  is equal to two. We have a basis of the space consisting of normalized eigenforms

$$E_k - p^{k-1}E_k^{(p)}, \quad E_k - E_k^{(p)}.$$

### 3 Bounds on congruences

Let  $k$  be an even positive integer and  $p$  be a rational prime. We want to find congruences between Eisenstein series  $E_k - p^{k-1}E_k^{(p)}$  and cuspidal newforms in the space  $\mathcal{M}_k(\Gamma_0(p))$ . Let  $f$  be a newform in  $\mathcal{S}_2(\Gamma_0(p))$ . Assume there exists a prime ideal  $\lambda$  in  $\mathcal{O}_f$  and a natural number  $r$  such that

$$a_n(E_k - p^{k-1}E_k^{(p)}) \equiv a_n(f) \pmod{\lambda^r}. \quad (4)$$

The bound on  $r$  depends on the  $q$ -expansion of the Eisenstein series at cuspidal points of the modular curve  $X_0(p)$ . The modular curve  $X_0(p)$  has two cusps, 0 and  $\infty$ . Hence for any modular form  $f \in \mathcal{M}_k(\Gamma_0(p))$  we have  $q$ -expansions at  $\infty$  and 0. We compute expansions for  $f$  and  $f|_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ . We denote by  $\mu(f)$  the zeroth coefficient of the  $q$ -expansion of the form  $f$  at 0. Equivalently, this is the zeroth coefficient of the  $q$ -expansion of the form  $f|_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  at  $\infty$ .

**Lemma 1.** *Let  $p$  be a prime number,  $k \geq 2$  be an even integer and  $f \in \mathcal{S}_k(\Gamma_0(p))$  be a newform. Let  $\lambda$  be a prime ideal in  $\mathcal{O}_f$  such that  $p \notin \lambda$  and let  $r \geq 1$  be a natural number. Let  $E$  denote the Eisenstein series  $E_k - p^{k-1}E_k^{(p)}$ . Suppose we have a congruence*

$$a_n(f) \equiv a_n(E) \pmod{\lambda^r} \quad (5)$$

for all  $n \geq 0$ . Then  $\mu(E) \equiv 0 \pmod{\lambda^r}$ . Hence the form  $E$  is cuspidal modulo  $\lambda^r$ .

*Proof.* For any even integer  $k \geq 2$  the formula

$$(E_k - p^{k-1}E_k^{(p)})|_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = E_k - \frac{1}{p}E_k^{(1/p)}$$

holds. It follows that  $\mu(E)$  equals  $-\frac{B_k}{2k} \left(1 - \frac{1}{p}\right)$ . By [1, Theorem 3] we have that

$$a_p(f) = -\varepsilon_p p^{k/2-1}$$

for some  $\varepsilon_p \in \{-1, 1\}$ . On the other side,  $a_p(E) = 1$ , hence  $-\varepsilon_p p^{k/2-1} \equiv 1 \pmod{\lambda^r}$  by (5). Thence, we obtain the congruence

$$1 - p^{k-2} \equiv 0 \pmod{\lambda^r}. \quad (6)$$

Observe that  $\mu(E) = -\frac{B_k}{2k}(1 - p^{k-2}) + \left(-\frac{B_k}{2k}(1 - p^{k-1})\right) \left(-\frac{1}{p}\right)$ . Since  $f$  is a cusp-form, the assumption (5) implies that  $a_0(E) \equiv 0 \pmod{\lambda^r}$ , hence  $-\frac{B_k}{2k}(1 - p^{k-1}) \equiv 0 \pmod{\lambda^r}$ . The last congruence and the congruence (6) imply that  $\mu(E) \equiv 0 \pmod{\lambda^r}$ .

**Corollary 1.** *Let  $p$  and  $\ell$  be two distinct rational primes. Suppose that we have two integers  $k \geq 2$ ,  $r \geq 1$  and  $k$  is even. Let  $f$  be a newform in  $\mathcal{S}_k(\Gamma_0(p))$ . Suppose that for  $E = E_k - p^{k-1}E_k^{(p)}$  we have congruences*

$$a_n(f) \equiv a_n(E) \pmod{\lambda^r}$$

for all  $n \geq 0$  and some prime ideal  $\lambda$  in  $\mathcal{O}_f$  dividing  $\ell$ . There is an upper bound

$$r \leq \text{ord}_\lambda(\ell) \cdot v_\ell \left( -\frac{B_k}{2k}(1 - p) \right),$$

where  $v_\ell$  denotes the  $\ell$ -adic valuation on  $\mathbb{Q}$ .

*Proof.* By Lemma 1 we have  $\mu(E) \equiv 0 \pmod{\lambda^r}$ , hence  $-\frac{B_k}{2k} \left(1 - \frac{1}{p}\right) \equiv 0 \pmod{\lambda^r}$ . Since  $p$  is invertible modulo  $\lambda$ , then

$$-\frac{B_k}{2k}(1 - p) \equiv 0 \pmod{\lambda^r}.$$

The exponent  $r$  satisfies the inequality  $r \leq \min(\text{ord}_\lambda(a_0(E)), \text{ord}_\lambda(\mu(E)))$ . But we have for  $k \geq 2$

$$\text{ord}_\lambda \left( -\frac{B_k}{2k}(1 - p^{k-1}) \right) \geq \text{ord}_\lambda \left( -\frac{B_k}{2k}(1 - p) \right),$$

hence

$$r \leq \text{ord}_\lambda(\ell) \cdot v_\ell \left( -\frac{B_k}{2k}(1 - p) \right).$$

*Remark 1.* Let  $p \in \lambda$  or equivalently  $p = \ell$ . For  $k > 2$  the congruence (6) (which holds either when  $p = \ell$  or when  $p \neq \ell$ ) implies that  $1 - \ell^{k-2} \in \lambda^r$ , hence  $1 - \ell^{k-2} \in \lambda$ , hence  $1 \in \lambda$ , which leads to a contradiction. If  $k = 2$ , we observe that  $a_0(E_2 - pE_2^{(p)}) \equiv 0 \pmod{\lambda^r}$ . Hence  $\text{ord}_\lambda(-\frac{1}{24}(1 - p)) \geq r \geq 1$ , so  $1 - p \in \lambda$  and  $1 \in \lambda$ , since  $\ell = p$ , which is impossible.

In the computations below we use a straightforward generalization of the well-known theorem of Sturm [19], suitable for our purposes. A similar theorem in more general form is proved in [4, Proposition 1].

**Theorem 1.** *Let  $p$  be a rational prime and  $k \geq 2$  be an even integer. Let  $f \in \mathcal{S}_k(\Gamma_0(p))$  be a normalized eigenform. Let  $\ell$  be a rational prime dividing the numerator of  $-\frac{B_k}{2k}(1 - p^{k-1})$ . Suppose we have a positive integer  $r$  and a nonzero prime ideal  $\lambda$  in  $\mathcal{O}_f$ , containing  $\ell$ , such that for all  $n \leq \frac{k(p+1)}{12}$  there is a congruence*

$$a_n(f) \equiv a_n(E_k - p^{k-1}E_k^{(p)}) \pmod{\lambda^r}.$$

*Then the congruence holds for all  $n \geq 0$ .*

*Proof.* Let us denote by  $B$  the number  $\frac{k(p+1)}{12}$  and by  $E$  the form  $E_k - p^{k-1}E_k^{(p)}$ . Let  $m$  denote the denominator of  $-\frac{B_k}{2k}(1 - p^{k-1})$ . Observe that  $\ell \nmid m$ . Fourier coefficients of the form  $mE$  are rational integers. Coefficients of the form  $f$  lie in  $\mathcal{O}_f$ . If  $r = 1$ , then we know that for  $n \leq B$

$$a_n(mf) \equiv a_n(mE) \pmod{\lambda},$$

hence by the theorem of Sturm (cf. [18, Theorem 9.18]) we get the congruence for all  $n \geq 0$ . But  $m \notin \lambda$ , hence

$$a_n(f) \equiv a_n(E) \pmod{\lambda}$$

for all  $n \geq 0$ . If  $r > 1$ , then we proceed by induction. Assume first that the statement is true for  $r - 1$ . Suppose that  $a_n(f) \equiv a_n(E) \pmod{\lambda^r}$  for  $n \leq B$ . In particular, we get  $a_n(f) \equiv a_n(E) \pmod{\lambda^{r-1}}$  for all  $n \geq 0$  by the induction hypothesis. Choose any algebraic integer  $\pi \in \lambda \setminus \lambda^2$ . Then the function  $\frac{1}{\pi^{r-1}}(f - E)$  is a modular form in  $\mathcal{M}_k(\Gamma_0(p))$  with Fourier coefficients lying in the localization  $(\mathcal{O}_f)_\lambda$  of the ring  $\mathcal{O}_f$  at the prime ideal  $\lambda$ . By the theorem of Shimura (cf. [17, Theorem 3.52]) the space  $\mathcal{S}_k(\Gamma_0(p))$  has a basis with the Fourier expansion in  $\mathbb{Z}$ . The same is true for  $\mathcal{M}_k(\Gamma_0(p))$ . Hence, there exists an algebraic integer  $\alpha \in \mathcal{O}_f \setminus \lambda$  such that  $\frac{\alpha}{\pi^{r-1}}(f - E)$  has the Fourier expansion in  $\mathcal{O}_f$ . Moreover, for all  $n \leq B$  the congruence

$$a_n\left(\frac{\alpha}{\pi^{r-1}}(f - E)\right) \equiv 0 \pmod{\lambda}$$

holds. By the Sturm theorem, it is true for all  $n \geq 0$ . This implies

$$a_n(\alpha(f - E)) \equiv 0 \pmod{\lambda^r}$$

for all  $n \geq 0$ . Since  $\alpha \notin \lambda$ , the induction step holds true and the theorem is proved.

## 4 Orders in number fields

Fix a rational prime  $\ell$ . In this section we introduce the concept of an  $\ell$ -maximal order. The content of this section is well-known, however we present the main theorems for the convenience of the reader. We follow the exposition of the subject presented in [5], [14] and [15]. We fix also an algebraic integer  $\theta$  and a number field  $K = \mathbb{Q}(\theta)$ .

**Definition 1.** An order in the number field  $K$  is a subring  $\mathcal{O} \subset K$  which is a finitely generated  $\mathbb{Z}$ -module of rank  $\deg(K)$ .

By  $\mathcal{O}_K$  we will denote the ring of algebraic integers in  $K$  or equivalently the maximal order in  $K$ .

**Definition 2.** An order  $\mathcal{O}$  in  $K$  is  $\ell$ -maximal if

$$\ell \nmid [\mathcal{O}_K : \mathcal{O}].$$

**Definition 3.** Let  $\mathcal{O}$  be an order in  $K$ . The  $\ell$ -radical of  $\mathcal{O}$  is the set

$$I_\ell(\mathcal{O}) = \{x \in \mathcal{O} : \exists_{m \geq 1} \quad x^m \in \ell \mathcal{O}\}.$$

**Lemma 2 ([5], Proposition 6.1.2).** *The  $\ell$ -radical is an ideal in  $\mathcal{O}$ . Moreover there is a decomposition*

$$I_\ell(\mathcal{O}) = \prod_i \mathfrak{L}_i$$

where the product runs over prime ideals  $\mathfrak{L}_i$  in  $\mathcal{O}$  lying over  $\ell$ .

**Lemma 3 ([5], Theorem 6.1.3).** *Let  $\mathcal{O}$  be an order in  $K$ . The set  $\mathcal{O}'$  which we define by*

$$\mathcal{O}' = \{x \in K : xI_\ell(\mathcal{O}) \subset I_\ell(\mathcal{O})\}$$

is an order in  $K$ . Either

$$\mathcal{O} = \mathcal{O}'$$

in which case  $\mathcal{O}$  is  $\ell$ -maximal, equivalently  $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$  or

$$\mathcal{O} \subsetneq \mathcal{O}'$$

and  $[\mathcal{O}' : \mathcal{O}] = \ell^n$  for some positive integer  $n$ .

Moreover, if  $\mathcal{O} = \mathcal{O}'$ , then

$$\mathcal{O} = \{x \in \mathcal{O}_K \mid \exists_{j \geq 1} \quad \ell^j x \in \mathcal{O}\}.$$

**Corollary 2.** *Let  $R_0$  be equal to  $\mathbb{Z}[\theta]$  and define the chain of rings*

$$R_i \subset R_{i+1}$$



by the condition  $R_{i+1} = R_i'$ . There exists an  $m$  such that the chain stabilizes

$$R_m = R_{m+1} = R_{m+2} = \cdots$$

and then

$$R_m = \{x \in \mathcal{O}_K \mid \exists j \geq 1 \quad \ell^j x \in \mathbb{Z}[\theta]\}.$$

*Proof.* By Lemma 3 it follows that for  $m$  such that  $R_m = R_{m+1}$  we have

$$R_m = \{x \in \mathcal{O}_K \mid \exists j \geq 1 \quad \ell^j x \in R_m\}.$$

Let  $L = \{x \in \mathcal{O}_K \mid \exists j \geq 1 \quad \ell^j x \in \mathbb{Z}[\theta]\}$  and  $x \in L$ . Then  $\ell^j x \in \mathbb{Z}[\theta]$  for some positive  $j$ . But  $\mathbb{Z}[\theta] = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_m$ . Therefore  $\ell^j x \in R_m$ , hence  $x \in R_m$ , proving  $L \subset R_m$ .

Let  $x \in R_m$ . Then  $x \in \mathcal{O}_K$ . By definition  $R_m = R_{m-1}' = \{x \in K \mid xI_\ell(R_{m-1}) \subset I_\ell(R_{m-1})\}$ . By Lemma 2 we have that  $I_\ell(R_{m-1}) = \prod_i \mathfrak{L}_i$ , primes  $\mathfrak{L}_i$  in  $R_{m-1}$  containing  $\ell$ . So there exists  $k \geq 1$  such that  $\ell^k \in I_\ell(R_{m-1})$ . So  $\ell^k x \in I_\ell(R_{m-1})$ , hence  $\ell^k x \in R_{m-1}$ . By induction we can show that there is a positive  $s$  such that  $\ell^s x \in \mathbb{Z}[\theta]$ , since  $R_0 = \mathbb{Z}[\theta]$ . It implies that

$$R_m \subset L.$$

This corollary thus shows how to construct an  $\ell$ -maximal order containing  $\mathbb{Z}[\theta]$ .

**Lemma 4 ([5], Proposition 4.8.15).** *Let  $\mathcal{O}$  be an order in  $K$  and  $\mathfrak{L}$  be a prime ideal in  $\mathcal{O}$ . Then there exists an  $a \in K \setminus \mathcal{O}$  such that  $a\mathfrak{L} \subset \mathcal{O}$ . Moreover,  $\mathfrak{L}$  is invertible if and only if  $a\mathfrak{L} \not\subset \mathfrak{L}$ .*

**Lemma 5.** *Let  $\mathcal{O}$  be an  $\ell$ -maximal order in  $K$ . Every prime ideal  $\mathfrak{L}$  in  $\mathcal{O}$  lying over  $\ell$  is invertible, i.e.  $\mathfrak{L}\mathfrak{L}^{-1} = \mathcal{O}$ .*

*Proof.* Let  $\mathfrak{L}$  be a prime ideal which is invertible in the  $\ell$ -maximal order  $\mathcal{O}$  and lies over  $\ell$ . By the previous lemma there exists an  $a \in K \setminus \mathcal{O}$  such that  $a\mathfrak{L} \subset \mathcal{O}$ .

The order  $\mathcal{O}$  is  $\ell$ -maximal so by Lemma 3

$$\mathcal{O} = \mathcal{O}' = \{x \in K : xI_\ell(\mathcal{O}) \subset I_\ell(\mathcal{O})\}.$$

Hence  $aI_\ell(\mathcal{O}) \not\subset I_\ell(\mathcal{O})$  and by Lemma 2

$$a \prod_i \mathfrak{L}_i \not\subset \prod_i \mathfrak{L}_i$$

where the product ranges over primes  $\mathfrak{L}_i$  in  $\mathcal{O}$  lying above  $\ell$ . Suppose that  $a\mathfrak{L} \subset \mathfrak{L}$ . Multiplication by other primes over  $\ell$  in  $\mathcal{O}$  implies that  $a \prod_i \mathfrak{L}_i \subset \prod_i \mathfrak{L}_i$ , which leads to a contradiction. Hence  $a\mathfrak{L} \not\subset \mathfrak{L}$  and  $\mathfrak{L}$  is invertible.

We will use the following fact which we prove due to the lack of the precise reference.

**Theorem 2.** *Let  $\mathcal{O}$  be an  $\ell$ -maximal order in  $K$ . We have a factorization into powers of prime ideals*

$$\ell\mathcal{O} = \prod_{i=1}^n \mathfrak{L}_i^{e_i}$$

and

$$\ell\mathcal{O}_K = \prod_{i=1}^n \mathcal{L}_i^{e_i}$$

with  $\mathcal{L}_i \cap \mathcal{O} = \mathfrak{L}_i$ .

*Proof.* The ideal  $\ell\mathcal{O}$  factors into a product of prime powers (cf. [5, Section 6.2.2])

$$\ell\mathcal{O} = \prod_i \mathfrak{L}_i^{e_i}. \quad (7)$$

On the other hand the ideal  $\ell\mathcal{O}_K$  splits as follows

$$\ell\mathcal{O}_K = \prod_j \mathcal{L}_j^{E_j}$$

in  $\mathcal{O}_K$ , where  $\mathcal{L}_j$  are prime ideals above  $\ell$  in  $\mathcal{O}_K$ . Every prime ideal  $\mathfrak{L}_i$  is invertible by Lemma 5. Hence, by [10, Theorem 11.4] the localization  $\mathcal{O}_{\mathfrak{L}_i}$  of the ring  $\mathcal{O}$  at the prime ideal  $\mathfrak{L}_i$ , is a discrete valuation ring. For any prime  $\mathfrak{L}$  above  $\ell$  in  $\mathcal{O}$ , the ideal  $\mathfrak{L}\mathcal{O}_K$  is prime in  $\mathcal{O}_K$  by [14, Proposition 12.10]. Moreover, the same proposition implies the equality of localizations  $\mathcal{O}_{\mathfrak{L}} = (\mathcal{O}_K)_{\mathfrak{L}\mathcal{O}_K}$ . The prime  $\mathfrak{L}\mathcal{O}_K$  is a unique prime ideal above  $\mathfrak{L}$  in  $\mathcal{O}_K$ . On the other side, if  $\mathcal{L}$  is a prime ideal above  $\ell$  in  $\mathcal{O}_K$ , then  $\mathcal{L} \cap \mathcal{O}$  is a prime ideal in  $\mathcal{O}$ . The mappings

$$\mathfrak{L} \mapsto \mathfrak{L}\mathcal{O}_K,$$

$$\mathcal{L} \cap \mathcal{O} \mapsto \mathcal{L}$$

establish a bijection between the sets of prime ideals above  $\ell$  in  $\mathcal{O}$  and in  $\mathcal{O}_K$ . We can now write  $\mathfrak{L}_i = \mathcal{L}_i \cap \mathcal{O}$  for any  $i$  in the product (7). We check that  $E_i = e_i$  for all  $i$ . Choose an index  $i$ . Then  $\ell\mathcal{O}_{\mathfrak{L}_i} = \mathfrak{L}_i^{e_i} \mathcal{O}_{\mathfrak{L}_i}$ , since  $\mathfrak{L}_i$  and  $\mathfrak{L}_j$  are coprime for  $i \neq j$ . Similarly,  $\ell(\mathcal{O}_K)_{\mathcal{L}_i} = \mathcal{L}_i^{E_i} (\mathcal{O}_K)_{\mathcal{L}_i}$ . The rings  $(\mathcal{O})_{\mathfrak{L}_i}$  and  $(\mathcal{O}_K)_{\mathcal{L}_i}$  are equal and are discrete valuation rings, hence  $E_i = e_i$ . The equality holds for any  $i$ , so the theorem is proved.

Finally, we can define a valuation on elements of an  $\ell$ -maximal order with respect to any prime ideal over  $\ell$ . For a nonzero prime ideal  $\mathfrak{L} \in \text{Spec } \mathcal{O}$  over  $\ell$ , let  $\mathcal{L} = \mathfrak{L}\mathcal{O}_K$  be the prime ideal in  $\mathcal{O}_K$ , which exists by the last theorem. Any element  $x \in \mathcal{O}$  can be written as

$$x = u_1 \pi^r = u_2 \Pi^r,$$

for  $u_1 \in \mathcal{O}_{\mathfrak{L}}^\times, u_2 \in (\mathcal{O}_K)_{\mathcal{L}}^\times$  and uniformizers  $\pi$  and  $\Pi$  in  $(\mathcal{O})_{\mathfrak{L}}$  and  $(\mathcal{O}_K)_{\mathcal{L}}$ , respectively. The common exponent of uniformizers will be denoted by

$$\text{ord}_{\mathfrak{L}}(x) := r.$$

The definition extends to  $K = \text{Frac}(\mathcal{O})$  by

$$\text{ord}_{\mathfrak{L}}\left(\frac{x}{y}\right) = \text{ord}_{\mathfrak{L}}(x) - \text{ord}_{\mathfrak{L}}(y).$$

The following equivalence holds for any  $x \in \mathcal{O} \subset \mathcal{O}_K$

$$\text{ord}_{\mathfrak{L}}(x) \geq r \Leftrightarrow x \equiv 0 \pmod{\mathcal{L}^r}.$$

In the algorithm presented below we use the last equivalence of orders. It is also crucial for the algorithm in Section 5 that the computation of an  $\ell$ -maximal order is more efficient than computation of the whole ring of algebraic integers which involves factorization of discriminants. By the result of Chistov (cf. [3, Theorem 1.3]), computation of the ring of algebraic numbers in the number field  $K$  is polynomially equivalent to finding the largest squarefree divisor of field discriminant. The latter problem has not found to date a satisfactory solution, better than just factorizing the whole integer. On the other hand, computation of an  $\ell$ -maximal order, as in Corollary 2, is straightforward and quick (cf. [5, Chapter 6]). Computation of prime ideals above  $\ell$  in an  $\ell$ -maximal order is equally fast, cf. [5, Chapter 6.2]. In our computations we often exploit this feature of  $\ell$ -maximal orders.

## 5 Sketch of the algorithm

Input:  $(p, k) \in \mathbb{Z}^2$ , where  $p$  is a prime number and  $k \geq 2$  is an even integer.

1. Compute Galois conjugacy classes of newforms in  $\mathcal{S}_k(\Gamma_0(p))$ . Call the set  $New$ .
2. Compute the Sturm bound  $B = \frac{k}{12} [SL_2(\mathbb{Z}) : \Gamma_0(p)] = \frac{k}{12} \cdot (p+1)$ .
3. Compute the coefficients  $a_n(E_k - p^{k-1}E_k^{(p)})$  for  $n \leq B$ .
4. Compute the set of primes  $L = \{\ell \text{ prime} : \ell \mid \text{Numerator}(-\frac{B}{2k}(1-p))\}$ .
5. For each pair  $(\ell, f) \in L \times New$ , compute  $K_f$ , i.e., the coefficient field of  $f$ . By  $f$  we mean here a choice of a representative in Galois conjugacy class.
6. Find an algebraic integer  $\theta$  such that  $K_f = \mathbb{Q}(\theta)$ .
7. Compute an  $\ell$ -maximal order  $\mathcal{O}$  above  $\mathbb{Z}[\theta]$  (see Corollary 2).
8. Compute the set  $\mathcal{S} = \{\lambda \in \text{Spec } \mathcal{O} : \lambda \cap \mathbb{Z} = \ell\mathbb{Z}\}$ .
9. For each  $\lambda \in \mathcal{S}$  compute

$$m_\lambda = \min_{n \leq B} (\text{ord}_\lambda(a_n(f) - a_n(E_k - p^{k-1}E_k^{(p)}))).$$

**Output:** If  $m_\lambda > 0$  then we have a congruence

$$a_n(f) \equiv a_n(E_k - p^{k-1}E_k^{(p)}) \pmod{(\lambda \mathcal{O}_f)^{m_\lambda}}$$

for all  $n \geq 0$ .

## 6 Numerical data

We present numerical data supporting the conjecture. The levels and ranges we have examined are summarized in Table 1

**Table 1** Range of computations

| k              | 2    | 4   | 6   | 8   | 10  | 12  | 14 | 16 | 18 | 20 | 22 |
|----------------|------|-----|-----|-----|-----|-----|----|----|----|----|----|
| prime $p \leq$ | 1789 | 397 | 229 | 193 | 109 | 113 | 97 | 71 | 67 | 67 | 59 |

In total, we found 740 congruences of the form (2) for the ranges and weights described above and a few that are outside of this range.

There are 67 congruences such that  $r > 1$ . We found around 110 congruences such that  $\lambda$  is ramified, i.e.  $\text{ord}_\lambda(\ell) > 1$ . Only 7 among them have the property that  $r > 1$ .

In the conjecture we have excluded a prime  $\ell = 2$  because we found two congruences for the level  $p = 257$ , weight  $k = 2$  and prime  $\ell = 2$  which provide example where the exponent  $r$  of the congruence is greater than  $\text{ord}_\lambda(\ell)$  and  $\text{ord}_\lambda(\ell) > 1$ . In Table 3 we present data concerning congruences for which  $\text{ord}_\lambda(\ell) = 1$ . In Table 4 we present cases where  $\text{ord}_\lambda(\ell) > 1$  and  $\text{ord}_\lambda(\mu(E)) > \text{ord}_\lambda(\ell)$ .

We are interested in a congruence of the type

$$a_n(E) \equiv a_n(f) \pmod{\lambda^r}$$

for all  $n \geq 0$ , between the Eisenstein series  $E = E_k - p^{k-1}E_k^{(p)} \in \mathcal{E}_k(\Gamma_0(p))$  and the newform  $f \in \mathcal{S}_k(\Gamma_0(p))$  for different weights  $k$  and prime levels  $p$ . We denote by  $d$  the degree of the number field  $K_f$  generated by the coefficients of the form  $f$  and  $\lambda$  is a prime ideal in the ring of integers of  $K_f$ , above the rational prime  $\ell \in \mathbb{Z}$ . The column labeled by  $nm$  contains the number of elements in the residue field associated with  $\lambda$ . Number  $e$  denotes the ramification of the ideal  $\lambda$  at  $\ell$  and  $m = \text{ord}_\lambda(\mu(E))$ . The column labeled by  $i$  contains the number of the Galois orbit of representing newform  $f$  (with respect to the internal MAGMA numbering).

Let  $k = 2$  and  $p = 1201$ . We find a newform  $f \in \mathcal{S}_2(\Gamma_0(1201))$  such that  $K_f = \mathbb{Q}(\sqrt{2})$  and

$$f = q - q^2 - q^4 + 2\sqrt{2}q^7 + 3q^8 - 3q^9 + (2 + \sqrt{2})q^{11} + \dots$$

We have the Eisenstein series

$$E_2 - 1201E_2^{(1201)} = 50 + \sum_{n=1}^{\infty} \sigma_1(n)q^n - 1201 \sum_{n=1}^{\infty} \sigma_1(n)q^{1201n}.$$

We check, by the algorithm, that for the prime ideal  $\lambda = (\sqrt{2})$

$$a_n(f) \equiv a_n(E_2 - 1201E_2^{(1201)}) \pmod{\lambda}$$

for all natural  $n \geq 0$ . We observe that the ideal  $(2) \in \mathcal{O}_f = \mathbb{Z}[\sqrt{2}]$  is totally ramified with  $(2) = \lambda^2$ . Moreover,  $a_{11}(E_2 - 1201E_2^{(1201)}) = 12$  and  $a_{11}(f) = 2 + \sqrt{2}$ , hence the maximal exponent  $r$  of the congruence is equal to 1. The upper bound proposed in the conjecture is equal to 2, so it is not always the case that the maximal exponent  $r$  is equal to that bound.

Let  $k = 2$  and  $p = 109$ . In this example we choose any root  $\alpha \in \overline{\mathbb{Q}}$  of the equation

$$\alpha^4 + \alpha^3 - 5\alpha^2 - 4\alpha + 3 = 0$$

and form  $K = \mathbb{Q}(\alpha)$ . We have the Galois conjugacy class of newforms with the  $q$ -expansion

$$f = q + \alpha q^2 + (1 + 4\alpha - \alpha^3)q^3 + (\alpha^2 - 2)q^4 - \alpha q^5 + \dots$$

The ring of integers  $\mathcal{O}_f$  of  $K_f = K$  is equal to  $\mathbb{Z}[\alpha]$  and

$$(3) = (3, \alpha)(3, 2 + \alpha + \alpha^2 + \alpha^3)$$

is the factorization into prime ideals in  $\mathcal{O}_f$ . We find, by the algorithm, that for  $\lambda = (3, \alpha)$

$$a_n(f) \equiv a_n(E_2 - 109E_2^{(109)}) \pmod{\lambda^2}$$

for all natural  $n \geq 0$ . In fact, this is the maximal possible exponent, since  $\mu(E_2 - 109E_2^{(109)}) = \frac{9}{2}$  and  $\text{ord}_\lambda(9) = 2$ . In the unramified case, the upper bound for the maximal exponent  $r$  is smaller or equal to the one described in Corollary 1. This example shows that we cannot have a smaller bound in general.

Let  $k = 8$  and  $p = 43$ . We choose any root  $\alpha \in \overline{\mathbb{Q}}$  of the equation

$$\begin{aligned} & -281015823360 + 26122731136\alpha + 25840429824\alpha^2 - 34580064\alpha^3 \\ & -584457696\alpha^4 - 13609592\alpha^5 + 5061216\alpha^6 + 169726\alpha^7 \\ & -18498\alpha^8 - 717\alpha^9 + 24\alpha^{10} + \alpha^{11} = 0 \end{aligned}$$

and form  $K = \mathbb{Q}(\alpha)$ . The ring of integers has the discriminant divisible exactly by 7. We have the Galois conjugacy class of newforms with the  $q$ -expansion

$$f = q + \alpha q^2 + a_3 q^3 + (\alpha^2 - 128)q^4 + \dots$$

It is congruent to a suitable Eisenstein series modulo a prime ideal above 7 which is ramified of exponent 2 and has a presentation

$$\lambda = \left(7, \frac{\beta}{3456}\right)$$

where

$$\begin{aligned}\beta = & 8448 + 43840\alpha + 38112\alpha^2 + 6248\alpha^3 + 7752\alpha^4 + 5918\alpha^5 \\ & + 2106\alpha^6 + 203\alpha^7 + 60\alpha^8 + \alpha^9.\end{aligned}$$

We get the congruence

$$a_n(f) \equiv a_n(E_8 - 43^7 E_8^{(43)}) \pmod{\lambda^2}$$

for all  $n \geq 0$  and the exponent is maximal, what confirms the conjecture.

Let  $k = 2$  and  $p = 3001$ . The space of cusp forms  $\mathcal{S}_2(\Gamma_0(3001))$  has dimension 249 and it is a direct sum of three subspaces  $S_1$ ,  $S_2$  and  $S_3$  of dimensions 2, 115 and 132, respectively. The space  $S_1$  is generated by two Galois conjugate newforms

$$f_1 = q + \alpha_1 q^2 + (\alpha_1 + 1)q^3 + (\alpha_1 - 1)q^4 + 2\alpha_1 q^5 + (2\alpha_1 + 1)q^6 + \dots,$$

$$f_2 = q + \alpha_2 q^2 + (\alpha_2 + 1)q^3 + (\alpha_2 - 1)q^4 + 2\alpha_2 q^5 + (2\alpha_2 + 1)q^6 + \dots,$$

where  $\alpha_1$  and  $\alpha_2$  are roots of the polynomial  $x^2 - x - 1$ . Since the forms are Galois conjugate, we will consider only one of them. Assume  $\alpha_1 = \frac{1+\sqrt{5}}{2}$ . The ring of integers of  $K_{f_1} = \mathbb{Q}(\sqrt{5})$  is  $\mathcal{O}_{f_1} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$  and

$$5\mathcal{O}_{f_1} = \lambda^2,$$

for the prime ideal  $\lambda$  which equals  $(5, 2 + \frac{1+\sqrt{5}}{2})$ . We check that  $a_0(E_2 - 3001E_2^{(3001)}) = 125$  and  $\mu(E_2 - 3001E_2^{(3001)}) = 125$ , and  $\text{ord}_\lambda(125) = 6$ . Corollary 1 predicts that the upper bound for the exponent  $r$  of the congruence is 6. We checked by MAGMA that for  $n \leq \frac{3001+1}{12}$  the congruence

$$a_n(f_1) \equiv a_n(E_2 - 3001E_2^{(3001)}) \pmod{\lambda}$$

holds. Hence, by Theorem 1 the congruence holds for all  $n \geq 0$ . But we also find that  $a_2(f_1) - a_2(E_2 - 3001E_2^{(3001)}) = \frac{1+\sqrt{5}}{2} - 3 \notin \lambda^2$ , which proves that the maximal exponent  $r$ , for which the congruence holds is equal to 1. It confirms the conjecture in this particular case.

If  $p = 163$  we obtain four different congruences for weights  $k = 2, 4, 6$  and 8 with ideals above 3 raised to the powers 3, 3, 2 and 3 respectively. For weights  $k = 2, 4$  or 8 the exponent of the ideal is maximal possible (cf. Table 3). For  $k = 2$  we find a number field of degree 7 over  $\mathbb{Q}$  with a primitive element  $\alpha$  with a minimal polyno-

mial

$$6 + 4\alpha - 23\alpha^2 + 19\alpha^4 - 5\alpha^5 - 3\alpha^6 + \alpha^7 = 0.$$

The ring of integers is equal to  $\mathbb{Z}[\alpha]$ . Its discriminant is equal to  $2 \cdot 82536739$  and

$$3\mathbb{Z}[\alpha] = (3, \alpha)(3, 1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6).$$

We find a newform of level 163 and weight 2 with  $q$ -expansion

$$f = q + \alpha q^2 + (-2 + 5\alpha + 5\alpha^2 - 6\alpha^3 - \alpha^4 + \alpha^5)q^3 \\ + (-2 + \alpha^2)q^4 + (6 + 6\alpha - 11\alpha^2 - 6\alpha^3 + 7\alpha^4 + \alpha^5 - \alpha^6)q^5 + \dots$$

It is congruent to the Eisenstein series

$$E_2 - 163E_2^{(163)} = \frac{27}{4} + \sum_{n=1}^{\infty} \sigma_1(n)q^n - 163 \sum_{n=1}^{\infty} \sigma_1(n)q^{163n}$$

modulo  $(3, \alpha)^3$ .

*Remark 2.* It is not always true that if we have a congruence modulo a power of a prime ideal above  $\ell$  and  $K_f = \mathbb{Q}(\theta)$ , where  $\theta$  is an algebraic integer, then an  $\ell$ -maximal order above  $\mathbb{Z}[\theta]$  that we get from the algorithm described in Corollary 2 is equal to the ring  $\mathbb{Z}[\theta]$ . We summarize several examples in Table 2. The prime  $\ell$  is unramified in  $K_f$ . By  $i$  we denote the number of the Galois orbit of the newform and by  $ind$  the index  $[\mathcal{O} : \mathbb{Z}[\theta]]$  for the  $\ell$ -maximal order above  $\mathbb{Z}[\theta]$ .

**Table 2** Index of the order

| p    | k | $\ell$ | i | ind |
|------|---|--------|---|-----|
| 101  | 6 | 5      | 2 | 625 |
| 751  | 2 | 5      | 2 | 625 |
| 1621 | 2 | 3      | 3 | 3   |
| 1667 | 2 | 7      | 2 | 343 |

From Table 3 we can read off many properties of the congruences satisfying  $ord_\lambda(\ell) = 1$ . For  $1 < r \leq ord_\lambda(\mu(E))$  we found only 5 congruences that do not satisfy  $r = ord_\lambda(\mu(E))$  and 56 that satisfy this condition. Observe that the exponent was not maximal only for  $k = 2$ . In all cases found, the residue degree was always equal to 1.

Moreover, if we fix  $r \geq 2$  and look for a newform satisfying the congruence (2) for  $r = ord_\lambda(\mu(E))$  and for a fixed Eisenstein series of level  $p$  we can find several examples for varying  $k$ , e.g. for  $p = 163$  or for 197.

An obvious necessary condition is that  $a_q(f) \equiv a_q(E) = q^{k-1} + 1 \pmod{\lambda^r}$  for prime  $q \neq p$ . To find a rational newform  $f$  as above, it is enough to look for an elliptic curve  $F$  (attached to  $f$  by the modularity theorem) defined over  $\mathbb{Q}$ , of prime conductor  $p$ , such that

**Table 3** Congruences with exponent greater than one and without ramification

| p    | k  | $\ell$ | r | m | i | d  | nm |
|------|----|--------|---|---|---|----|----|
| 769  | 2  | 2      | 5 | 5 | 2 | 36 | 2  |
| 1459 | 2  | 3      | 5 | 5 | 3 | 71 | 3  |
| 257  | 4  | 2      | 4 | 4 | 1 | 28 | 2  |
| 641  | 2  | 2      | 4 | 4 | 2 | 33 | 2  |
| 1409 | 2  | 2      | 4 | 4 | 3 | 65 | 2  |
| 163  | 2  | 3      | 3 | 3 | 3 | 7  | 3  |
| 163  | 4  | 3      | 3 | 3 | 1 | 19 | 3  |
| 163  | 8  | 3      | 3 | 3 | 1 | 46 | 3  |
| 193  | 2  | 2      | 3 | 3 | 3 | 8  | 2  |
| 193  | 6  | 2      | 3 | 3 | 2 | 41 | 2  |
| 251  | 2  | 5      | 3 | 3 | 2 | 17 | 5  |
| 449  | 2  | 2      | 3 | 3 | 2 | 23 | 2  |
| 487  | 2  | 3      | 3 | 4 | 4 | 16 | 3  |
| 577  | 2  | 2      | 3 | 3 | 4 | 18 | 2  |
| 811  | 2  | 3      | 3 | 3 | 3 | 40 | 3  |
| 1373 | 2  | 7      | 3 | 3 | 3 | 60 | 7  |
| 1601 | 2  | 2      | 3 | 3 | 2 | 80 | 2  |
| 1783 | 2  | 3      | 3 | 3 | 2 | 82 | 3  |
| 97   | 2  | 2      | 2 | 2 | 2 | 4  | 2  |
| 97   | 6  | 2      | 2 | 2 | 2 | 21 | 2  |
| 97   | 10 | 2      | 2 | 2 | 2 | 37 | 2  |
| 101  | 2  | 5      | 2 | 2 | 2 | 7  | 5  |
| 101  | 6  | 5      | 2 | 2 | 2 | 24 | 5  |
| 101  | 10 | 5      | 2 | 2 | 2 | 41 | 5  |
| 109  | 2  | 3      | 2 | 2 | 3 | 4  | 3  |
| 109  | 4  | 3      | 2 | 2 | 1 | 12 | 3  |
| 109  | 8  | 3      | 2 | 2 | 1 | 30 | 3  |
| 109  | 10 | 3      | 2 | 2 | 2 | 42 | 3  |
| 151  | 2  | 5      | 2 | 2 | 3 | 6  | 5  |
| 151  | 6  | 5      | 2 | 2 | 2 | 35 | 5  |
| 163  | 6  | 3      | 2 | 2 | 2 | 35 | 3  |
| 193  | 4  | 2      | 2 | 2 | 1 | 23 | 2  |
| 197  | 2  | 7      | 2 | 2 | 3 | 10 | 7  |
| 197  | 4  | 7      | 2 | 2 | 1 | 22 | 7  |
| 251  | 4  | 5      | 2 | 2 | 1 | 24 | 5  |
| 379  | 2  | 3      | 2 | 2 | 2 | 18 | 3  |
| 379  | 4  | 3      | 2 | 2 | 1 | 44 | 3  |
| 433  | 2  | 3      | 2 | 2 | 4 | 16 | 3  |
| 491  | 2  | 7      | 2 | 2 | 3 | 29 | 7  |
| 601  | 2  | 5      | 2 | 2 | 2 | 29 | 5  |
| 673  | 2  | 2      | 2 | 2 | 3 | 24 | 2  |
| 677  | 2  | 13     | 2 | 2 | 4 | 35 | 13 |
| 727  | 2  | 11     | 2 | 2 | 2 | 36 | 11 |
| 751  | 2  | 5      | 2 | 3 | 2 | 38 | 5  |
| 757  | 2  | 3      | 2 | 2 | 2 | 33 | 3  |
| 883  | 2  | 7      | 2 | 2 | 2 | 39 | 7  |
| 929  | 2  | 2      | 2 | 2 | 3 | 47 | 2  |
| 1051 | 2  | 5      | 2 | 2 | 3 | 48 | 5  |
| 1151 | 2  | 5      | 2 | 2 | 3 | 68 | 5  |
| 1153 | 2  | 2      | 2 | 4 | 3 | 50 | 2  |
| 1201 | 2  | 5      | 2 | 2 | 3 | 51 | 5  |
| 1217 | 2  | 2      | 2 | 3 | 2 | 58 | 2  |
| 1301 | 2  | 5      | 2 | 2 | 3 | 66 | 5  |
| 1451 | 2  | 5      | 2 | 2 | 2 | 73 | 5  |
| 1453 | 2  | 11     | 2 | 2 | 2 | 63 | 11 |
| 1471 | 2  | 7      | 2 | 2 | 2 | 72 | 7  |
| 1567 | 2  | 3      | 2 | 2 | 4 | 69 | 3  |
| 1601 | 2  | 5      | 2 | 2 | 2 | 80 | 5  |
| 1621 | 2  | 3      | 2 | 3 | 3 | 70 | 3  |
| 1667 | 2  | 7      | 2 | 2 | 2 | 82 | 7  |
| 1697 | 2  | 2      | 2 | 2 | 2 | 77 | 2  |

$$|\tilde{F}_q(\mathbb{F}_q)| \equiv 0 \pmod{\ell^r},$$

where  $\tilde{F}_q$  denotes a reduction of  $F$  at prime  $q$ . It follows by [9, Theorem 2], that there exists an elliptic curve  $F'$  over  $\mathbb{Q}$  which is  $\mathbb{Q}$ -isogenous to  $F$  and the group of  $\mathbb{Q}$ -rational points on  $F'$  contains a point of order  $\ell^r$ . The conductor of  $F'$  is  $p$ . For an elliptic curve defined over  $\mathbb{Q}$  the smallest possible conductor is 11. Hence  $F'$  has good reduction at 2. The group of  $\mathbb{Q}$ -rational points of  $F'$  contains the torsion subgroup, which we denote by  $T$ . The reduction at 2 maps  $T$  into  $\tilde{F}'_2(\mathbb{F}_2)$ . The kernel of this homomorphism has order a power of 2. The Hasse theorem for elliptic curves implies that  $|\tilde{F}'_2(\mathbb{F}_2)| \leq 5$ . Hence, the order  $|T|$  equals  $2^m$ ,  $2^m \cdot 3$  or  $2^m \cdot 5$ , for some  $m \geq 0$ . Suppose that  $|T| > 2$ .

If  $|T| = 2^m$ , then [12, Theorem 2] and [12, Theorem 3] imply that  $T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  or  $T \cong \mathbb{Z}/4\mathbb{Z}$  and in both cases  $p = 17$ . The only  $\mathbb{Q}$ -isogeny class of elliptic curves of conductor 17 is attached to the newform  $f = q - q^2 - q^4 + \dots$  in  $\mathcal{S}_2(\Gamma_0(17))$ . For any



prime  $q \neq p$  the coefficient  $a_q(f) = 1 + q - |\tilde{F}'_q(\mathbb{F}_q)|$  is congruent to  $1 + q$  modulo 4. We check directly that  $a_p(f) = 1$ . The congruence  $a_n(f) \equiv a_n(E_2 - 17E_2^{(17)}) \pmod{4}$  holds for all  $n \geq 1$ . However,  $a_0(E_2 - 17E_2^{(17)}) = \frac{2}{3}$ , so for all  $n \geq 0$  we have only a congruence modulo 2.

If  $|T| = 2^m \cdot 3$ , then [12, Theorem 1] implies that  $T \cong \mathbb{Z}/3\mathbb{Z}$  and  $p = 19$  or  $p = 37$ . There is exactly one  $\mathbb{Q}$ -isogeny class of elliptic curves of conductor 19. It provides the newform  $f = q - 2q^3 - 2q^4 + \dots$  in  $\mathcal{S}_2(\Gamma_0(19))$  congruent to  $E_2 - 19E_2^{(19)}$  modulo 3 at all coefficients. If the conductor  $p$  equals 37, then there are two  $\mathbb{Q}$ -isogeny classes of elliptic curves. Only the class associated with the newform  $f = q + q^3 - 2q^4 + \dots$  in  $\mathcal{S}_2(\Gamma_0(37))$  provides the congruence  $a_n(f) \equiv a_n(E_2 - 37E_2^{(37)}) \pmod{3}$  for all  $n \geq 0$ . The other newform  $f'$  satisfies  $a_p(f') = -1$ , so the congruence cannot hold.

If  $|T| = 2^m \cdot 5$ , then by [12, Theorem 4] we get  $T \cong \mathbb{Z}/5\mathbb{Z}$  and  $p = 11$ . The unique newform  $f \in \mathcal{S}_2(\Gamma_0(11))$  satisfies  $a_p(f) = 1$ . Moreover,  $a_0(E_2 - 11E_2^{(11)}) = \frac{5}{12}$ , hence the congruence  $a_n(f) \equiv a_n(E_2 - 11E_2^{(11)}) \pmod{5}$  holds for all  $n \geq 0$ .

We are left with only one case, when  $|T|$  equals 2. If the elliptic curve  $F'$  of prime conductor  $p > 17$  satisfies  $|T| = 2$ , then  $p = u^2 + 64$  for some rational number  $u$ . This is proved in [16, Theorem 2]. The primes  $p = 113, 353, 593$  and  $1153$  are of the form  $u^2 + 64$  for  $u \in \mathbb{Z}$  and on these levels we find newforms  $f \in \mathcal{S}_2(\Gamma_0(p))$  congruent congruent to  $E_2 - pE_2^{(p)}$  modulo 2. However, in general it is not known whether the sequence  $\{u^2 + 64\}_{u \in \mathbb{N}}$  contains an infinite number of primes.

In Table 4 we collect data about all congruences for which  $\text{ord}_\lambda(\ell) > 1$  and  $\text{ord}_\lambda(\mu(E)) > \text{ord}_\lambda(\ell)$ . For primes  $\ell \geq 3$  we found only 5. The cases when  $\text{ord}_\lambda(\mu(E))$  equals  $\text{ord}_\lambda(\ell)$  are presented in Table 5.

**Table 4** Congruences with  $m > e$  and with ramification

| p    | k | $\ell$ | r | m  | e  | i | d   | nm |
|------|---|--------|---|----|----|---|-----|----|
| 3001 | 2 | 5      | 1 | 6  | 2  | 1 | 2   | 5  |
| 3001 | 2 | 5      | 1 | 9  | 3  | 3 | 132 | 5  |
| 251  | 6 | 5      | 1 | 6  | 2  | 2 | 59  | 5  |
| 919  | 2 | 3      | 2 | 4  | 2  | 3 | 47  | 3  |
| 919  | 4 | 3      | 2 | 4  | 2  | 1 | 105 | 3  |
| 257  | 2 | 2      | 1 | 25 | 5  | 2 | 14  | 2  |
| 257  | 2 | 2      | 5 | 10 | 2  | 2 | 14  | 2  |
| 353  | 2 | 2      | 1 | 10 | 5  | 4 | 14  | 2  |
| 577  | 2 | 2      | 1 | 6  | 2  | 4 | 18  | 2  |
| 1153 | 2 | 2      | 1 | 16 | 4  | 3 | 50  | 2  |
| 1249 | 2 | 2      | 1 | 26 | 13 | 3 | 59  | 2  |
| 1601 | 2 | 2      | 1 | 6  | 2  | 2 | 80  | 2  |

| p    | k | $\ell$ | r | m  | e  | i | d   | nm |
|------|---|--------|---|----|----|---|-----|----|
| 1217 | 2 | 2      | 1 | 39 | 13 | 2 | 58  | 2  |
| 1889 | 2 | 2      | 1 | 4  | 2  | 3 | 96  | 2  |
| 2113 | 2 | 2      | 1 | 15 | 5  | 2 | 91  | 2  |
| 2273 | 2 | 2      | 1 | 10 | 5  | 3 | 105 | 2  |
| 257  | 4 | 2      | 1 | 12 | 3  | 1 | 28  | 2  |
| 257  | 4 | 2      | 1 | 16 | 4  | 2 | 36  | 2  |
| 257  | 4 | 2      | 1 | 20 | 5  | 1 | 28  | 2  |
| 257  | 4 | 2      | 1 | 20 | 5  | 2 | 36  | 2  |
| 257  | 4 | 2      | 1 | 20 | 5  | 2 | 36  | 2  |
| 257  | 4 | 2      | 1 | 8  | 2  | 1 | 28  | 2  |
| 257  | 4 | 2      | 5 | 8  | 2  | 1 | 28  | 2  |

*Remark 3.* The main difficulty in enlarging the number of congruences in Table 4 lies in the fact that  $\dim \mathcal{S}_k(\Gamma_0(p)) = O(k \cdot p)$  as  $k \rightarrow \infty$  and  $p \rightarrow \infty$ . In a typical

situation, when  $f \in \mathcal{S}_k(\Gamma_0(p))$  is a newform, the degree  $[K_f : \mathbb{Q}]$  is roughly of the size  $\frac{1}{2} \dim \mathcal{S}_k(\Gamma_0(p))$ . To check the congruence, we perform Step 9 of the algorithm in Section 5. We have to compute  $\frac{k}{12}(p+1)$  coefficients of the newform  $f$  and this is usually the slowest part of the algorithm. For example, when  $k = 2$  and  $p > 3000$ , this means that we work with the field  $K_f$  of degree at least 150 over  $\mathbb{Q}$ . In the range described in Table 1 we found all possible congruences such that  $\text{ord}_\lambda(\ell) > 1$ . For levels and weights bigger than those described in Table 1, we have decided to look only for congruences such that  $[K_f : \mathbb{Q}] < 100$ . This condition guarantees that Step 9 of the algorithm can be executed in less than 48 hours of computational time on the computer with Intel i5, 2.53 GHz processor and 4GB RAM.

**Table 5** Congruences with  $m = e$  and with ramification

| p   | k  | $\ell$ | r | m | e | i | d  | nm | p    | k  | $\ell$ | r | m | e | i | d  | nm  |
|-----|----|--------|---|---|---|---|----|----|------|----|--------|---|---|---|---|----|-----|
| 31  | 2  | 5      | 1 | 2 | 2 | 1 | 2  | 5  | 661  | 2  | 11     | 1 | 2 | 2 | 3 | 29 | 11  |
| 31  | 6  | 5      | 1 | 2 | 2 | 2 | 8  | 5  | 683  | 2  | 11     | 1 | 2 | 2 | 3 | 31 | 11  |
| 31  | 10 | 5      | 1 | 2 | 2 | 2 | 13 | 5  | 691  | 2  | 5      | 1 | 2 | 2 | 2 | 33 | 5   |
| 31  | 14 | 5      | 1 | 2 | 2 | 2 | 18 | 5  | 733  | 2  | 61     | 1 | 2 | 2 | 4 | 32 | 61  |
| 31  | 18 | 5      | 1 | 2 | 2 | 2 | 23 | 5  | 761  | 2  | 5      | 1 | 2 | 2 | 3 | 41 | 5   |
| 31  | 22 | 5      | 1 | 2 | 2 | 2 | 28 | 5  | 761  | 2  | 19     | 1 | 2 | 2 | 3 | 41 | 19  |
| 47  | 10 | 23     | 1 | 2 | 2 | 2 | 20 | 23 | 881  | 2  | 2      | 1 | 2 | 2 | 2 | 46 | 2   |
| 47  | 12 | 23     | 1 | 2 | 2 | 1 | 18 | 23 | 911  | 2  | 7      | 1 | 2 | 2 | 3 | 53 | 7   |
| 47  | 16 | 23     | 1 | 2 | 2 | 1 | 26 | 23 | 941  | 2  | 5      | 1 | 2 | 2 | 2 | 50 | 5   |
| 47  | 20 | 23     | 1 | 2 | 2 | 1 | 34 | 23 | 971  | 2  | 5      | 1 | 2 | 2 | 2 | 55 | 5   |
| 53  | 6  | 13     | 1 | 2 | 2 | 2 | 12 | 13 | 1021 | 2  | 17     | 1 | 2 | 2 | 2 | 47 | 17  |
| 53  | 18 | 13     | 1 | 2 | 2 | 2 | 38 | 13 | 1091 | 2  | 5      | 1 | 2 | 2 | 3 | 62 | 5   |
| 67  | 4  | 11     | 1 | 2 | 2 | 1 | 7  | 11 | 1201 | 2  | 2      | 1 | 2 | 2 | 1 | 2  | 2   |
| 67  | 14 | 11     | 1 | 2 | 2 | 2 | 37 | 11 | 1279 | 2  | 3      | 1 | 2 | 2 | 2 | 64 | 3   |
| 103 | 2  | 17     | 1 | 2 | 2 | 2 | 6  | 17 | 1289 | 2  | 7      | 1 | 2 | 2 | 4 | 61 | 7   |
| 113 | 2  | 2      | 1 | 2 | 2 | 2 | 2  | 2  | 1291 | 2  | 5      | 1 | 2 | 2 | 2 | 62 | 5   |
| 113 | 6  | 2      | 1 | 2 | 2 | 1 | 21 | 2  | 1381 | 2  | 5      | 1 | 2 | 2 | 2 | 63 | 5   |
| 113 | 6  | 2      | 1 | 2 | 2 | 1 | 21 | 4  | 1447 | 2  | 241    | 1 | 2 | 2 | 2 | 71 | 241 |
| 113 | 6  | 2      | 1 | 2 | 2 | 2 | 25 | 2  | 1471 | 2  | 5      | 1 | 2 | 2 | 2 | 72 | 5   |
| 113 | 6  | 2      | 1 | 2 | 2 | 2 | 25 | 2  | 1483 | 2  | 13     | 1 | 2 | 2 | 4 | 67 | 13  |
| 127 | 2  | 7      | 1 | 2 | 2 | 2 | 7  | 7  | 1511 | 2  | 5      | 1 | 2 | 2 | 2 | 87 | 5   |
| 127 | 8  | 7      | 1 | 2 | 2 | 1 | 34 | 7  | 1531 | 2  | 3      | 1 | 2 | 2 | 4 | 73 | 3   |
| 131 | 2  | 5      | 1 | 2 | 2 | 2 | 10 | 5  | 1531 | 2  | 5      | 1 | 2 | 2 | 4 | 73 | 5   |
| 131 | 6  | 5      | 1 | 2 | 2 | 2 | 32 | 5  | 1553 | 2  | 2      | 1 | 2 | 2 | 2 | 74 | 2   |
| 191 | 6  | 5      | 1 | 2 | 2 | 2 | 46 | 5  | 1693 | 2  | 3      | 1 | 2 | 2 | 3 | 72 | 3   |
| 199 | 2  | 3      | 1 | 2 | 2 | 3 | 10 | 3  | 1697 | 2  | 53     | 1 | 2 | 2 | 2 | 77 | 53  |
| 199 | 4  | 3      | 1 | 2 | 2 | 1 | 20 | 3  | 1777 | 2  | 2      | 1 | 2 | 2 | 2 | 79 | 2   |
| 211 | 2  | 5      | 1 | 2 | 2 | 1 | 2  | 5  | 1789 | 2  | 149    | 1 | 2 | 2 | 2 | 80 | 149 |
| 211 | 6  | 5      | 1 | 2 | 2 | 2 | 47 | 5  | 101  | 4  | 5      | 1 | 3 | 3 | 1 | 9  | 5   |
| 223 | 4  | 37     | 1 | 2 | 2 | 1 | 24 | 37 | 101  | 8  | 5      | 1 | 3 | 3 | 1 | 26 | 5   |
| 281 | 2  | 5      | 1 | 2 | 2 | 2 | 16 | 5  | 101  | 12 | 5      | 1 | 3 | 3 | 1 | 42 | 5   |
| 307 | 4  | 3      | 1 | 2 | 2 | 1 | 35 | 3  | 181  | 2  | 5      | 1 | 3 | 3 | 2 | 9  | 5   |
| 337 | 2  | 2      | 1 | 2 | 2 | 2 | 15 | 2  | 181  | 6  | 5      | 1 | 3 | 3 | 2 | 40 | 5   |
| 337 | 4  | 7      | 1 | 2 | 2 | 1 | 40 | 7  | 353  | 4  | 2      | 1 | 3 | 3 | 1 | 40 | 2   |
| 353 | 4  | 2      | 1 | 2 | 2 | 2 | 48 | 2  | 1321 | 2  | 11     | 1 | 3 | 3 | 4 | 56 | 11  |
| 353 | 4  | 11     | 1 | 2 | 2 | 1 | 40 | 11 | 1381 | 2  | 23     | 1 | 3 | 3 | 2 | 63 | 23  |
| 367 | 4  | 61     | 1 | 2 | 2 | 1 | 41 | 61 | 1571 | 2  | 5      | 1 | 3 | 3 | 2 | 82 | 5   |
| 401 | 4  | 5      | 1 | 2 | 2 | 1 | 45 | 5  | 1747 | 2  | 3      | 1 | 3 | 3 | 3 | 77 | 3   |
| 409 | 2  | 17     | 1 | 2 | 2 | 2 | 20 | 17 | 1201 | 2  | 2      | 1 | 5 | 5 | 3 | 51 | 2   |
| 409 | 4  | 17     | 1 | 2 | 2 | 1 | 47 | 17 | 353  | 4  | 2      | 1 | 5 | 5 | 1 | 40 | 2   |
| 419 | 4  | 19     | 1 | 2 | 2 | 1 | 43 | 19 | 353  | 4  | 2      | 1 | 5 | 5 | 2 | 48 | 2   |
| 523 | 2  | 3      | 1 | 2 | 2 | 3 | 26 | 3  | 353  | 4  | 2      | 1 | 5 | 5 | 2 | 48 | 2   |
| 541 | 2  | 5      | 1 | 2 | 2 | 2 | 24 | 5  | 353  | 4  | 2      | 2 | 2 | 2 | 1 | 40 | 2   |
| 571 | 2  | 5      | 1 | 2 | 2 | 9 | 18 | 5  | 43   | 8  | 7      | 2 | 2 | 2 | 1 | 11 | 7   |
| 593 | 2  | 2      | 1 | 2 | 2 | 5 | 27 | 2  | 43   | 20 | 7      | 2 | 2 | 2 | 1 | 32 | 7   |

## Acknowledgments

The author would like to thank Wojciech Gajda for many helpful suggestions and corrections. He thanks Gerhard Frey for reading an earlier version of the paper and for helpful comments and remarks. He would like to thank Gabor Wiese for his help in improving the paper and suggesting one of the lemmas. Finally, the author wishes to express his thanks to an anonymous referee for the careful reading of the paper and a detailed list of comments which improved the exposition and removed several inaccuracies.

## References

1. A. O. L. Atkin and J. Lehner, *Hecke operators on  $\Gamma_0(m)$* , Math. Ann. **185** (1970), 134–160.
2. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
3. J. A. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260.
4. I. Chen, I. Kiming, and J.B. Rasmussen, *On congruences mod  $p^m$  between eigenforms and their attached Galois representations.*, J. Number Theory **130** (2010), no. 3, 608–619.
5. H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
6. F. Diamond and J. Shurman, *A first course in modular forms.*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.
7. L. Dieulefait and X. Taixés i Ventosa, *Congruences between modular forms and lowering the level mod  $l^n$* , J. Théor. Nombres Bordeaux **21** (2009), no. 1, 109 – 118.
8. X. Taixés i Ventosa and G. Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers.*, Arithmetic, geometry, cryptography and coding theory 2009, Contemp. Math. **521** (2010), 145–166.
9. Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502.
10. Hideyuki Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid.
11. B. Mazur, *Modular curves and the Eisenstein ideal.*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33 – 186.
12. Isao Miyawaki, *Elliptic curves of prime power conductor with  $\mathbf{Q}$ -rational points of finite order*, Osaka J. Math. **10** (1973), 309–323. MR 0327776 (48 #6118)
13. B. Naskręcki, *Algorithm*, <http://bnaskrecki.faculty.wmi.amu.edu.pl/doku.php/magma>.
14. Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
15. M. E. Pohst, *Computational algebraic number theory.*, DMV Seminar, vol. 21, Birkhäuser Verlag, Basel, 1993.
16. Bennett Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367–378.
17. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1.

18. William Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by Paul E. Gunnells.
19. J. Sturm, *On the congruence of modular forms.*, Lecture Notes in Math. (1987), no. 1240, 275–280.